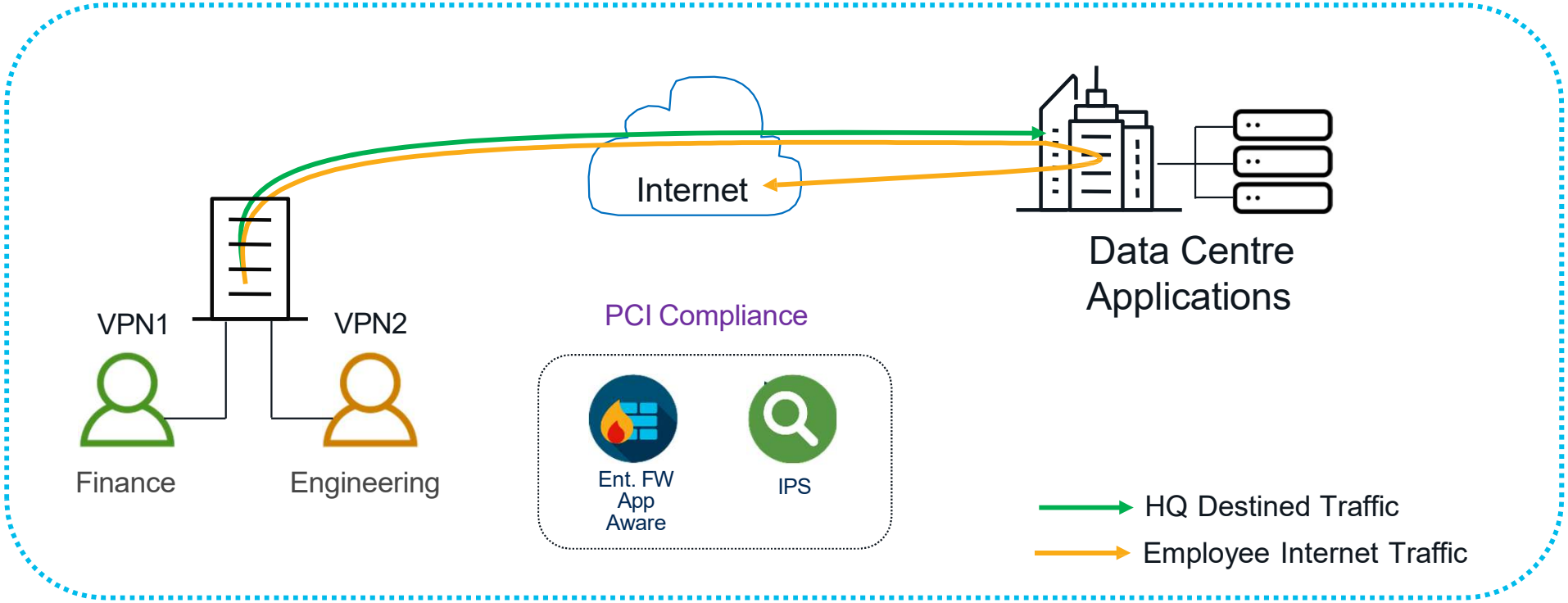
Zone Based Firewall

Controller Mode ✓

Autonomous Mode ✓

Zone Based Firewall Use Case: PCI Compliance



Zone Based Firewall – Benefits and Requirements

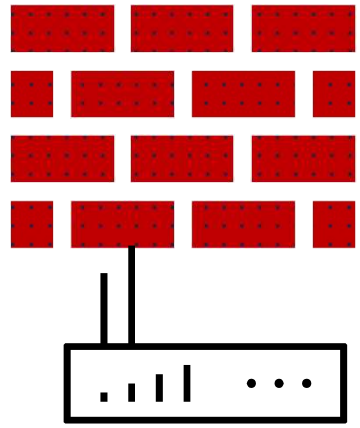
Benefits

- PCI * compliance
- Stateful firewall built into branch routers
- VLAN Segmentation
- Supports VRF
- Supports IPv6

* PCI – Payment Card Industry

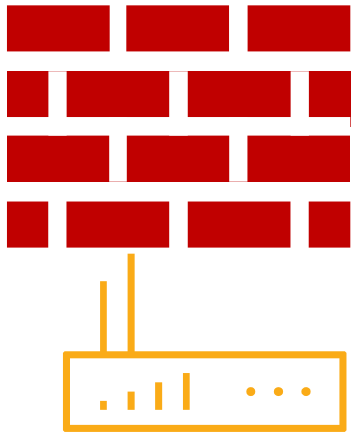
Requirements

- SEC-K9 license or
- Cisco DNA Network Essentials (Catalyst 8000)
- XE 3.9 and above on ISR 4K
- XE 16.6.1 and above on ISR 1K
- XE 16.6.1 and above on ISRv
- XE 3.7S and above on ASR1K
- XE 3.10S and above on CSR 1000V
- XE 17.3.2 and above for C8300 and C8500
- XE 17.4.1 and above for C8500L, C8200 and 8000V

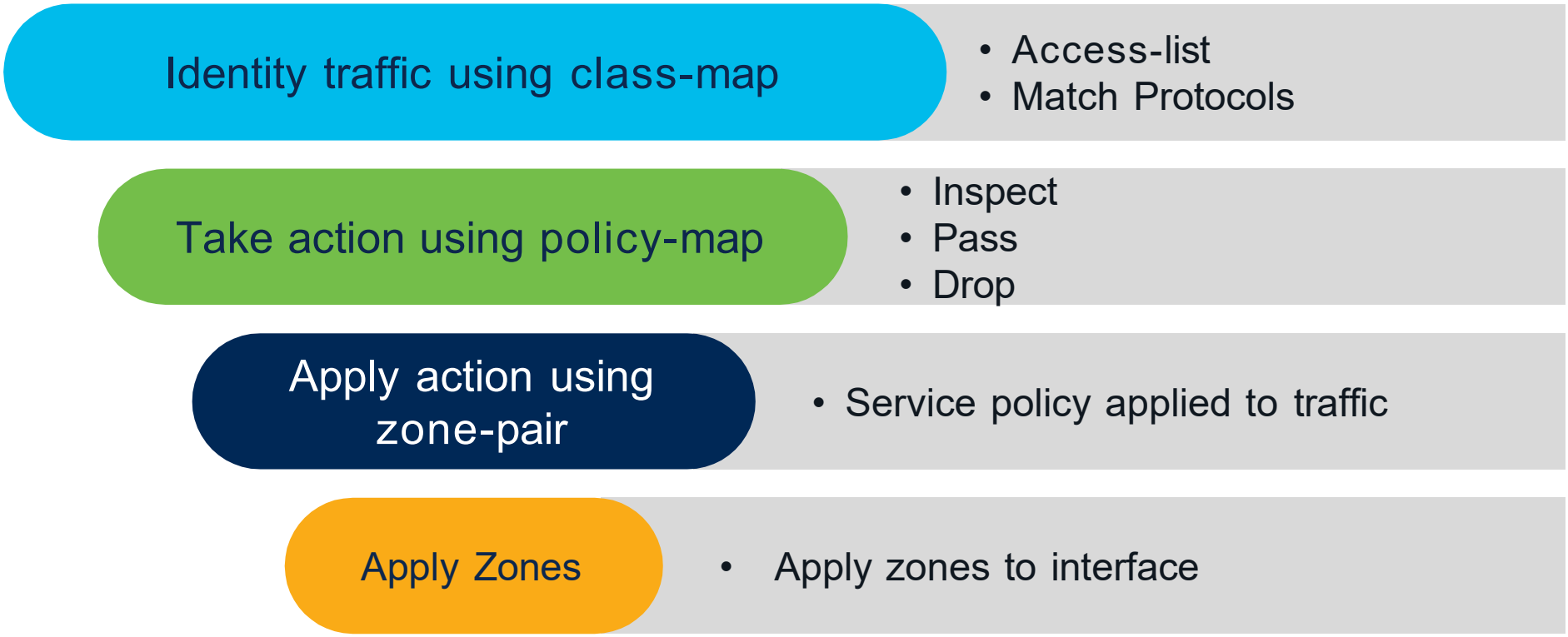


Zone Based Firewall

- Custom Zone
- default zone
  - “default” security zone for all INSIDE interfaces
  - default zone has always been in IOS-XE
  - default zone support on ISR-G2 is from 15.6(1)T
- Self Zone



Zone Based Firewall - Configuration



Zone Based Firewall - Custom Zone

Theory - directional, different policy based on packet direction

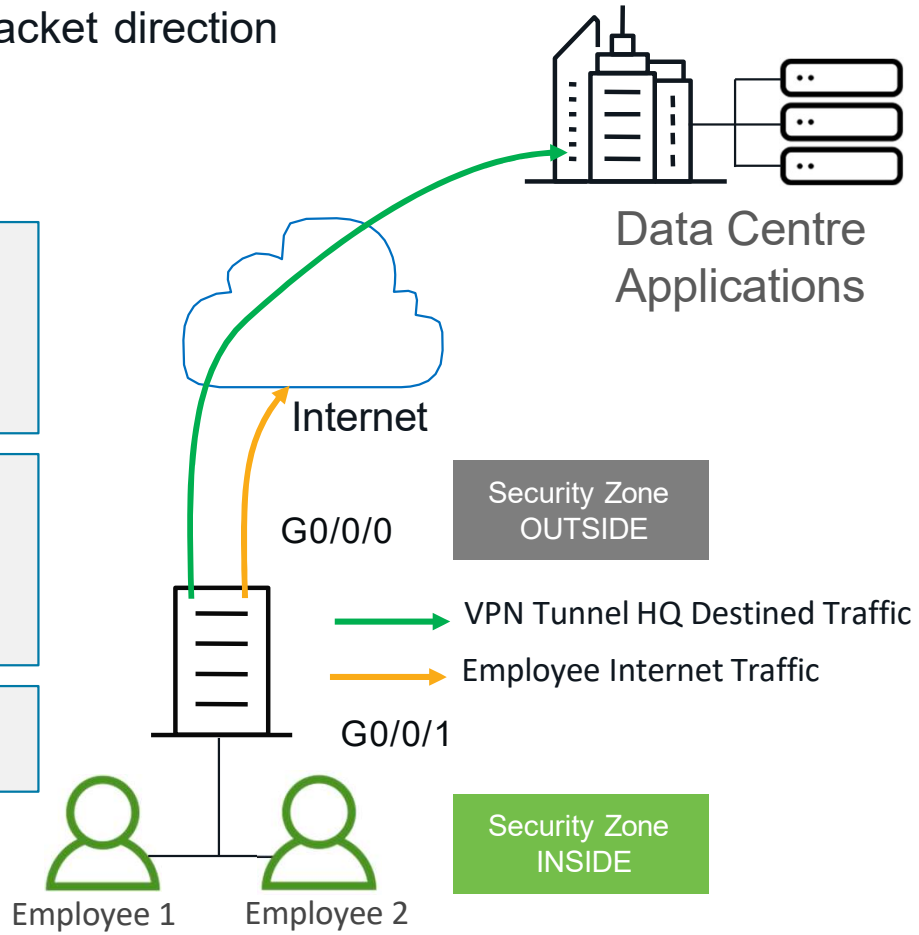
```
zone security INSIDE
zone security OUTSIDE
```

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp                    | or match access-list
 match protocol udp
 match protocol icmp
```

```
policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
 class type inspect INSIDE-TO-OUTSIDE-CLASS
 inspect
 class class-default
  drop
```

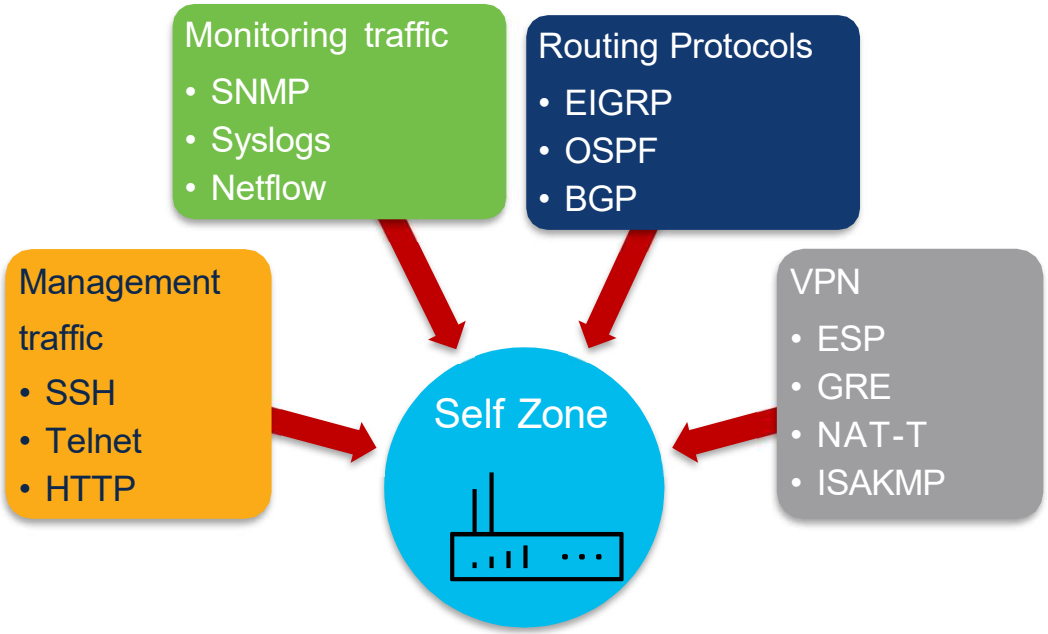
```
zone-pair security IN_OUT source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
```

```
Interface G0/0/0
 zone-member security OUTSIDE
Interface G0/0/1
 zone-member security INSIDE
```



Zone Based Firewall – Self Zone

- Pre-defined zone member
  - Protects traffic TO and FROM router
  - Traffic sourced or destined to router
  - Excludes THROUGH the box NAT traffic
- Two differences
  - Pre-defined and available for use
  - Explicit allow compared to explicit deny
- Use to protect management and control plane traffic



Zone Based Firewall

Self Zone inbound - Inbound traffic to the router itself

```
ip access-list extended ACL-RTR-IN
 permit udp host y.y.y.y any eq 4500
 permit udp host y.y.y.y any any eq isakmp
 permit icmp host x.x.x.x any echo
 permit icmp host x.x.x.x any echo-reply
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit udp any any range 33434 33463 ttl eq 1
```

```
ip access-list extended ESP-IN
 permit esp host x.x.x.x any

ip access-list extended DHCP-IN
 permit udp any eq bootps any eq bootpc

ip access-list extended GRE-IN
 permit gre host x.x.x.x any
```

```
class-map type inspect match-any INSPECT-ACL-IN-CLASS
 match access-group name ACL-RTR-IN

class-map type inspect match-any PASS-ACL-IN-CLASS
 match access-group name ESP-IN
 match access-group name DHCP-IN
 match access-group name GRE-IN

policy-map type inspect ACL-IN-POLICY
 class type inspect INSPECT-ACL-IN-CLASS
 inspect
 class type inspect PASS-ACL-IN-CLASS
   pass
 class class-default
   drop
```

```
zone-pair security TO-ROUTER source OUTSIDE destination self
  service-policy type inspect ACL-IN-POLICY
```

Zone Based Firewall

Self Zone outbound – Outbound traffic from the router itself

```
ip access-list extended ACL-RTR-OUT
 permit udp any host y.y.y.y eq 4500
 permit udp any host y.y.y.y eq isakmp
 permit icmp any host y.y.y.y
```

```
ip access-list extended ESP-OUT
 permit esp any host y.y.y.y

ip access-list extended DHCP-OUT
 permit udp any eq bootpc any eq bootps
```

```
class-map type inspect match-any INSPECT-ACL-OUT-CLASS
 match access-group name ACL-RTR-OUT

class-map type inspect match-any PASS-ACL-OUT-CLASS
 match access-group name ESP-OUT
 match access-group name DHCP-OUT

 policy-map type inspect ACL-OUT-POLICY
  class type inspect INSPECT-ACL-OUT-CLASS
  inspect
 class type inspect PASS-ACL-OUT-CLASS
   pass
 class class-default
  drop
```

```
zone-pair security FROM-ROUTER source self destination OUTSIDE
 service-policy type inspect ACL-OUT-POLICY
```

Firewall App Aware – Benefits and Requirements

Benefits

- Application Visibility and Granular control
- 1694+ layer 7 applications classified
- Allow or block traffic by application, category, application-family or application-group
- Segmentation
- PCI compliance
- Supports VRF and IPv6

Requirements

- SEC-K9 license or
- Cisco DNA Network Essentials (Catalyst 8000)
- XE 3.9 and above on ISR 4K
- XE 16.6.1 and above on ISR 1K
- XE 16.6.1 and above on ISRv
- XE 3.7S and above on ASR1K
- XE 3.10S and above on CSR 1000V
- XE 17.3.2 and above for C8300 and C8500
- XE 17.4.1 and above for C8500L, C8200 and 8000V

Firewall App Aware - Configuration

```
zone security INSIDE
zone security OUTSIDE
```

```
class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS
 match protocol ftp
 match protocol tcp     [AND / OR] match access-group name
 match protocol udp
 match protocol icmp
```

```
class-map match-any AVC-CLASS
 match protocol yahoo
 match protocol amazon
 match protocol attribute category consumer-streaming
 match protocol attribute category gaming
 match protocol attribute category social-networking
```

```
policy-map type inspect avc AVC-POLICY
 class AVC-CLASS
  deny
 class class-default
  allow
```

```
policy-map type inspect INSIDE-TO-OUTSIDE-POLICY
 class type inspect INSIDE-TO-OUTSIDE-CLASS
 inspect
   service-policy avc AVC-POLICY
 class class-default
  drop
```

```
zone-pair security IN_OUT source INSIDE destination
          OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE-POLICY
```

```
Interface G0/0/0
 zone security OUTSIDE
Interface G0/0/1
 Zone security INSIDE
```